IN THE CLAIMS

Please amend the claims as follows:

Claims 1-15 (Canceled).

Claim 16 (New): A denial-of-service attack detecting system for detecting a denial-of-service attack on a communication device, the denial-of-service attack detecting system comprising:

a monitoring device that monitors a packet transmitted to a communication device that is a target of the denial-of-service attack;

a performance measuring device that measures performance of the communication device; and

an attack determining device that performs communication with the monitoring device and the performance measuring device, wherein

the monitoring device includes a traffic abnormality detecting unit that detects traffic abnormality information indicating an abnormality of traffic due to the packet with respect to the communication device,

the performance measuring device includes a performance abnormality detecting unit that detects performance abnormality information indicating an abnormality of throughput of the communication device, and

the attack determining device includes an effects determining unit that determines whether the communication device received the denial-of-service attack, based on the traffic abnormality information and the performance abnormality information.

Claim 17 (New): The denial-of-service attack detecting system according to claim 16, wherein

the monitoring device further includes a traffic-abnormality-information transmitting unit that transmits the traffic abnormality information to the attack determining device.

Claim 18 (New): The denial-of-service attack detecting system according to claim 16, wherein

the performance measuring device further includes a performance-abnormality-information transmitting unit that transmits the performance abnormality information to the attack determining device.

Claim 19 (New): The denial-of-service attack detecting system according to claim 16, wherein

the traffic abnormality detecting unit detects the traffic abnormality information based on a predetermined attack detection condition that is set in advance.

Claim 20 (New): The denial-of-service attack detecting system according to claim 19, wherein

the monitoring unit further includes a signature generating unit that generates a signature indicating a feature of the packet attacking the communication device, based on the attack detection condition, and

the traffic abnormality information includes the signature.

Claim 21 (New): The denial-of-service attack detecting system according to claim 16, wherein

the traffic abnormality detecting unit detects the traffic abnormality information based on a steady traffic indicating an average traffic of the packet transmitted to the communication device.

Claim 22 (New): The denial-of-service attack detecting system according to claim 16, wherein

the performance abnormality detecting unit detects the performance abnormality information based on a predetermined performance abnormality detection condition that is set in advance.

Claim 23 (New): The denial-of-service attack detecting system according to claim 22, wherein

the performance abnormality detection condition includes

a response time from transmission of a response request message to the communication device to reception of a response message corresponding to the response request message, and

number of times that the response time exceeds a predetermined threshold.

Claim 24 (New): The denial-of-service attack detecting system according to claim 16, wherein

the performance abnormality detecting unit detects the performance abnormality information based on a steady performance indicating an average performance feature of the communication device.

Claim 25 (New): The denial-of-service attack detecting system according to claim 16, wherein

the effects determining unit determines that the communication device received the denial-of-service attack, when it is determined that one of the traffic abnormality information and the performance abnormality information causes an occurrence of other of the traffic abnormality information and the performance abnormality information based on an abnormality occurrence time included in the traffic abnormality information and the performance abnormality information.

Claim 26 (New): The denial-of-service attack detecting system according to claim 16, wherein

when the effects determining unit determines that the communication device received the denial-of-service attack, the attack determining device transmits the traffic abnormality information and the performance abnormality information used for the determination to a device for reporting to an operator.

Claim 27 (New): The denial-of-service attack detecting system according to claim 16, wherein

each of the traffic abnormality information and the performance abnormality information includes a certificate, and

the effects determining unit determines whether the communication device received the denial-of-service attack, after performing an authorization based on certificates.

Claim 28 (New): A method of detecting a denial-of-service attack on a communication device by using a monitoring device that monitors a packet transmitted to a communication device that is a target of the denial-of-service attack, a performance measuring device that measures performance of the communication device, and an attack determining device that performs communication with the monitoring device and the performance measuring device, the method comprising:

traffic abnormality detecting including the monitoring device detecting traffic abnormality information indicating an abnormality of traffic due to the packet with respect to the communication device;

performance abnormality information detecting including the performance measuring device detecting performance abnormality information indicating an abnormality of throughput of the communication device; and

effects determining including the attack determining device determining whether the communication device received the denial-of-service attack, based on the traffic abnormality information and the performance abnormality information.

Claim 29 (New): The method according to claim 28, further comprising:

traffic abnormality information transmitting including the monitoring device transmitting the traffic abnormality information to the attack determining device.

Claim 30 (New): The method according to claim 28, further comprising:

performance abnormality information transmitting including the performance measuring device transmitting the performance abnormality information to the attack determining device.